UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

JACLYN MOORE, Individually and on Behalf of All Others Similarly Situated,	:	Hon. Joseph H. Rodriguez
Plaintiff,	:	Civil Action No. 17-6266
v.	:	OPINION
HIGHPOINT SOLUTIONS LLC and CHRISTINE M. CUSHMAN,	:	
Defendants.	:	

This matter is before the Court on motion of Defendant Highpoint Solutions LLC ("HighPoint") to dismiss the Complaint pursuant to Fed. R. Civ. P. 12(b)(1) and 12(b)(6). The Court has considered the submissions of the parties and heard oral argument on May 30, 2018. For the reasons placed on the record that day, as well as those articulated below, the motion will be granted.

Background

Plaintiff Jaclyn Moore, a HighPoint contract employee since April 2017, has filed a purported Class Action Complaint as the result of a data breach by Defendant Christine M. Cushman, who was HighPoint's Human Resource Director.

On August 7, 2017, the Montgomery County, Pennsylvania District Attorney's office and certain news outlets announced that Cushman had stolen approximately one million dollars from HighPoint over a two-year period using private financial information HighPoint maintained concerning subcontractors. Specifically, from May 5, 2015 to June 15, 2017, Cushman used this stolen information to issue herself 45 fraudulent checks totaling $919,301.[1]

[1] The press release provided:

> NORRISTOWN, Pa. (Aug. 7, 2017)—Montgomery County District Attorney Kevin R. Steele and East Norriton Township Police Chief Karyl J. Kates announce the arrest of Christine Cushman, 31, of Douglassville, Pa., on felony charges of Theft by Unlawful Taking, Receiving Stolen Property and Identity Theft for stealing $919,301 from her employer, HighPoint Solutions LLC, in East Norriton.
>
> HighPoint Solutions was alerted to the potential thefts by its payroll company, after a bank officer had noticed suspicious multiple direct deposits of significant size going into the defendant's personal account. The company's chief financial officer met with East Norriton Township Detective Anthony Caso on July 4, 2017, about the potential theft. The ensuing investigation revealed that Cushman, who was HighPoint Solutions' director of human resources, was issuing fraudulent payroll checks in the names of four former subcontractors who no longer did business with the company. Cushman's responsibilities included preparing and reviewing the payroll information before it was submitted to the outside payroll company. The 45 thefts occurred between May 5, 2015 and June 15, 2017 and totaled $919,301.
>
> "Nearly $1 million was stolen from this company by a senior-

On August 8, 2017, HighPoint's CEO John Seitz emailed HighPoint's employees concerning Cushman's actions. The e-mail provided:

> Colleagues,
>
> By now many of you are aware of the press release from the Pennsylvania District Attorney and subsequent articles regarding Christine Cushman, our former HR Manager. HighPoint indeed was the victim of a corporate theft over the past two years. The details are available in numerous online articles—I've attached the most thorough one I've found below.
>
> http://www.readingeagle.com/news/article/amity-township-woman-stole-nearly-1-million-from-employer-police-say
>
> The purpose of my email is to explain the actions we have taken, as well as inform you of any risks to the company and employees' personal and financial information. By all evidence we've seen, HighPoint was the only victim in this theft, as funds were stolen from our bank account. No client, employee, or subcontractor bank account ever received or had any funds withdrawn. Once informed, we took appropriate remediation steps—including notifying the authorities.
>
> We have hired an independent, national audit firm to perform a forensic audit of our financial records and our controls to ensure no further damage has occurred beyond what we've found, as well as to help strengthen our financial oversight. Although the amount stolen was indeed significant, I can assure you we are a profitable and financially sound company.

> level, trusted employee. This breach of trust is something that needs to be guarded against by other companies," said Steele. "Unfortunately, corporate theft is all too prevalent and requires a system of checks and balances within the corporate system to make sure this doesn't happen."

(Compl. ¶ 14.)

> For our employees, as I mentioned, all evidence points to only a HighPoint bank account being involved in this theft. However, please understand that our HR Department does have on file (and Ms. Cushman had access to) all employee Social Security information as well as bank account information for those using direct deposit. At this time, we don't know if employee personal information was also stolen. Please be on alert for any suspicious activity relating to your personal and financial records.
>
> For those customers who ask, please make clear to them that Ms. Cushman did not have access to customer information/invoicing, and we believe there is no risk to customer identity information. We can also assure them that we are a financially sound partner and that we will be filing an insurance claim for this matter.
>
> Finally, we are coordinating all activities and communications strictly with the authorities, and I would ask all employees to refrain from participating in any social media discussions relating to this matter.
>
> Thank you for your patience and understanding during this process.
>
> Sincerely,
> John Seitz, Chief Executive Officer
> HighPoint Solutions, LLC

(Compl. ¶ 15.)

Seitz e-mailed HighPoint's employees again on August 10, 2017, as follows:

> As a follow up to my Tuesday email regarding the risk of compromise to our employee information (i.e. the "Cushman matter"), we have purchased a corporate-wide LifeLock identity protection subscription for all employees to help monitor and protect each employee's individual financial records. We have

purchased a 12-month plan that covers each U.S.-based employee, plus spouse and 1 child. Ms. Cushman had no involvement in ex-U.S. payroll processing, so we feel the U.S. focus covers all relevant risk. The corporate subscription will take a few days to activate, and we will be sending sign-up directions once available.

In addition, we are communicating the events and our remediation plan to our clients on a case-by-case basis. If you are aware of a customer who has raised concerns about this matter, please direct that inquiry to a HighPoint executive, as we are replying directly to those clients one-on-one. For your benefit, our message to those clients is as follows:

- Once aware of the theft, we took immediate action, including notifying local law enforcement authorities
- As a $170M revenue company, this theft obviously hurt, but in no way affects our standing as a profitable and financially strong partner. We have also submitted an insurance claim to recover most of the loss
- This breach occurred within our HR payroll operations, specific to sub-contractors—separated from our client financial operations that includes timesheet management, project management and invoicing
- We have hired a nationally-accredited audit firm to perform a thorough review of our financial controls and to perform a forensic audit of our financial records

Thank you for your continued patience as we continue to sort out and resolve this matter.

Regards,
John Seitz, Chief Executive Officer
HighPoint Solutions, LLC

(Compl. ¶ 16.)

As a result of the data breach, Plaintiff has alleged that Defendants negligently failed:

> to secure and safeguard her personal identifying information ("PII"), and that of, at least, all of HighPoint's past and current employees, agents, subcontractors, customers and service providers, as well as their families and dependents (the "Class"). This PII includes, but is not limited to, the: names, Social Security numbers, Taxpayer Identification Numbers, birthdates, addresses, telephone numbers, email addresses, healthcare records, salary and bonus details, contract and agreement details, sensitive employment information such as performance evaluations, disciplinary and employment termination details, severance packages, and/or other personal information concerning HighPoint's past and current employees, agents, subcontractors, customers and service providers, as well as their families and dependents. HighPoint was also negligent in failing to provide timely and adequate notice to Plaintiff and the Class that their PII had been stolen and precisely what types of information were stolen.

(Compl. ¶ 3.) Against HighPoint, the Complaint alleges negligence, intrusion upon seclusion, breach of fiduciary duty, breach of contract, breach of implied contract, violation of the New Jersey Computer Related Offenses Act, and vicarious liability. There is an additional claim for unjust enrichment against Cushman. HighPoint seeks dismissal of the Complaint.

Motion to Dismiss Standard

Rule 12(b)(1) of the Federal Rules of Civil Procedure permits the dismissal of an action for "lack of subject matter jurisdiction." "A motion to dismiss for want of standing is also properly brought pursuant to Rule 12(b)(1), because standing is a jurisdictional matter." Ballentine v. United States, 486 F.3d 806, 810 (3d Cir. 2007). "The party invoking federal

jurisdiction bears the burden of establishing the elements of standing, and each element must be supported in the same way as any other matter in which the plaintiff bears the burden of proof, i.e., with the manner and degree of evidence required at the successive stages of the litigation." Focus v. Allegheny Cnty. Court of Common Pleas, 75 F.3d 834, 838 (3d Cir. 1996) (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992)).

A Rule 12(b)(1) motion may be treated as either a facial or factual challenge to the court's subject matter jurisdiction. Davis v. Wells Fargo, 824 F.3d 333, 346 (3d Cir. 2016). A facial attack contests the sufficiency of the pleadings, whereas a factual attack contests the sufficiency of jurisdictional facts. Lincoln Ben. Life Co. v. AEI Life, LLC, 800 F.3d 99, 105 (3d Cir. 2015). When considering a facial attack, the court accepts the plaintiff's well-pleaded factual allegations as true and draws all reasonable inferences from those allegations in the plaintiff's favor. In re Horizon Healthcare Services Inc. Data Breach Litigation, 846 F.3d 625, 633 (3d Cir. 2017). When reviewing a factual attack, the court may weigh and consider evidence outside the pleadings. Gould Elecs. Inc. v. United States, 220 F.3d 169, 176 (3d Cir. 2000).

Federal Rule of Civil Procedure 12(b)(6) permits a motion to dismiss "for failure to state a claim upon which relief can be granted[.]" For a

complaint to survive dismissal under Rule 12(b)(6), it must contain sufficient factual matter to state a claim that is plausible on its face. Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)). A claim is facially plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. Further, a plaintiff must "allege sufficient facts to raise a reasonable expectation that discovery will uncover proof of her claims." Connelly v. Lane Const. Corp., 809 F.3d 780, 789 (3d Cir. 2016). In evaluating the sufficiency of a complaint, district courts must separate the factual and legal elements. Fowler v. UFMC Shadyside, 578 F.3d 203, 210-11 (3d Cir. 2009) ("Iqbal ... provides the final nail-in-the-coffin for the 'no set of facts' standard that applied to federal complaints before Twombly."). The Court "must accept all of the complaint's well-pleaded facts as true," Fowler, 578 F.3d at 210, "and then determine whether they plausibly give rise to an entitlement for relief." Connelly, 809 F.3d at 787 (citations omitted). Restatements of the elements of a claim, however, are legal conclusions and, therefore, not entitled to a presumption of truth. Burtch v. Milberg Factors, Inc., 662 F.3d 212, 224 (3d Cir. 2011).

Discussion

Plaintiff has conceded through briefing that her claims for breach of contract and breach of implied contract cannot survive and are voluntarily dismissed. Accordingly, the remaining claims are for negligence[2] and breach of fiduciary duty, intrusion upon seclusion,[3] violation of the New Jersey Computer Related Offenses Act,[4] and vicarious liability.[5]

---

[2] Under New Jersey law, to prove negligence, the plaintiff must establish: (1) a duty of care owed to the plaintiff by the defendant; (2) that defendant breached that duty of care; and (3) that plaintiff's injury was proximately caused by defendant's breach. Smith v. Kroesen, 9 F. Supp. 3d 439, 442 (D.N.J. 2014) (citing Endre v. Arnold, 692 A.2d 97 (N.J. Super Ct. App. Div. 1997)).

[3] Intrusion upon seclusion occurs when a plaintiff can show (i) an intentional intrusion (ii) upon the seclusion of another that is (iii) highly offensive to a reasonable person. In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 293 (3d Cir. 2016), cert. denied sub nom. C. A. F. v. Viacom Inc., 137 S. Ct. 624 (2017).

[4] Under the New Jersey Computer Related Offenses Act, a person or enterprise is liable for: "The purposeful or knowing, and unauthorized altering, damaging, taking or destruction of any data, data base, [etc.]; . . . The purposeful or knowing accessing and reckless altering, damaging, destroying or obtaining of any data, data base, [etc.]." N.J. Stat. Ann. § 2A:38A-3.

[5] An employer may be vicariously liable for its employee's act within the scope of her employment: (1) if the act is of the kind she is employed to perform; (2) if it occurs substantially within the authorized time and space limits; (3) if it is actuated, at least in part, by a purpose to serve the employer; and (4) if force is intentionally used by the employee against another, the use of force is not unexpectable by the employer. Davis v. Devereux Found., 37 A.3d 469, 489-90 (N.J. 2012).

The Constitution limits the subject matter jurisdiction of federal courts to "cases" and "controversies." See U.S. Art. III § 2. To establish Article III standing, a plaintiff must plead "an 'injury in fact' or an 'invasion of a legally protected interest that is concrete and particularized,' . . . a 'causal connection between the injury and the conduct complained of,' and 'a likelihood that the injury will be redressed by a favorable decision.'" In re Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 633 (3d Cir. 2017) (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992)). See also Anjelino v. N.Y. Times Co., 200 F.3d 73, 88 (3d Cir. 2000) ("Standing is established at the pleading stage by setting forth specific facts that indicate that the party has been injured in fact or that injury is imminent, that the challenged action is causally connected to the actual or imminent injury, and that the injury may be redressed by the cause of action.").

The Supreme Court has made clear that an "injury in fact" must be "concrete," which means "it must actually exist." Spokeo Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016). "Concrete" injuries may be "intangible" or non-economic, but, like other cognizable injuries, they must be "actual or imminent, not conjectural or hypothetical." Spokeo, 136 S. Ct. at 1548. See also Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) ("threatened

injury must be certainly impending to constitute injury in fact," and "[a]llegations of possible future injury" are not sufficient); Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (finding, in a data security breach case, "[a]llegations of 'possible future injury' are not sufficient to satisfy Article III").

To determine whether an intangible harm is sufficiently concrete, a court must first decide "whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." Spokeo, 136 S. Ct. at 1549. If so, "it is likely to be sufficient to satisfy the injury-in-fact element of standing." Horizon, 846 F.3d at 637. Next, the court determines "whether Congress has expressed an intent to make an injury redressable;" for, "even if an injury was previously inadequate in law, Congress may elevate it to the status of [a] legally cognizable injur[y]." Id. (quoting Spokeo, 846 F.3d at 637). Even in the context of a statutory violation, however, Article III standing requires a concrete injury. Spokeo, 136 S. Ct. at 1549.

Applying Spokeo, the Third Circuit denied a facial challenge in a Fair Credit Reporting Act case where plaintiff alleged that two laptop computers containing unencrypted personal information of over 800,000 health insurance customers were stolen from the defendant's headquarters.

Horizon, 846 F.3d at 630. Among the stolen data was names, addresses, member identification numbers, dates of birth, "and in some instances, a Social Security Number and/or limited clinical information." Id. The breach led to a fraudulent tax return filed in plaintiff's name and to an attempted credit card fraud. Plaintiff was also "denied retail credit because his social security number has been associated with identity theft." Id.

The Third Circuit held that the alleged injuries were sufficiently "concrete" to confer constitutional standing. First, under Anglo–American law, "unauthorized disclosures of information have long been seen as injurious." Id. at 638. "The common law alone will sometimes protect a person's right to prevent the dissemination of private information . . . [and] improper dissemination of information can itself constitute a cognizable injury." Id. at 638-39. Second, by passing the FCRA, Congress clearly intended to establish "that the unauthorized dissemination of personal information by a credit reporting agency causes an injury in and of itself—whether or not the disclosure of that information increased the risk of identity theft or some other future harm." Id. at 639.

The Court limited it holding as follows:

> We are not suggesting that Horizon's actions would give rise to a cause of action under common law. No common law tort proscribes the release of truthful information that is not harmful to one's reputation or otherwise offensive. But with the

> passage of FCRA, Congress established that the unauthorized dissemination of personal information by a credit reporting agency causes an injury in and of itself—whether or not the disclosure of that information increased the risk of identity theft or some other future harm. It created a private right of action to enforce the provisions of FCRA, and even allowed for statutory damages for willful violations—which clearly illustrates that Congress believed that the violation of FCRA causes a concrete harm to consumers. And since the "intangible harm" that FCRA seeks to remedy "has a close relationship to a harm [i.e. invasion of privacy] that has traditionally been regarded as providing a basis for a lawsuit in English or American courts," Spokeo, 136 S. Ct. at 1549, we have no trouble concluding that Congress properly defined an injury that "give[s] rise to a case or controversy where none existed before." Id. (citation and internal quotation marks omitted).

Horizon, 846 F.3d at 639-40. Here, Plaintiff has not pled a violation of FCRA or another statute that may be read to create standing by its mere violation, as in Horizon. As such, traditional concepts of standing guide the Court's analysis. See Reilly, 664 F.3d at 41-43 ("Constitutional standing requires an injury-in-fact, which is an invasion of a legally protected interest that is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical. . . . [A]llegations of an increased risk of identity theft resulting from a security breach are therefore insufficient to secure standing.").

In this case, the Court finds that Plaintiff has failed to allege facts demonstrating that she has sustained a concrete injury in fact. Any allegation of an increased risk of identity theft is speculative and

conclusory. Plaintiff has pled no facts to indicate that her personal identifying information was even accessed by Cushman, but more importantly, Plaintiff has failed to allege actual misuse of her personal identifying information.

Other courts in this District have held that plaintiffs who similarly alleged that personal information was lost or compromised, without asserting misuse, lacked standing to bring claims following data breaches. See Polanco v. Omnicell, Inc., 988 F. Supp. 2d 451 (D.N.J. 2013) (stating that "the Third Circuit expressly determined in Reilly that the 'alleged time and money expenditures [of the plaintiffs] to monitor their financial information [did] not establish standing . . . because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than the allege 'increased risk of injury' which form[ed] the basis for' the plaintiffs' claims"); Hinton v. Heartland Payment Sys., Inc., No. 09-594, 2006 WL 2177036, at *1 (D.N.J. Mar. 16, 2009); Giordano v. Wachovia Sec., LLC, No. 06-476, 2006 WL 2177036, at *4-5 (D.N.J. July 31, 2006) ("The mere possibility of future harm fails to satisfy the standing requirements of the Supreme Court and the Third Circuit Court of Appeals."). See also Storm v. Paytime, Inc., 90 F. Supp. 3d 359 (M.D. Pa. 2015) ([T]he Third Circuit requires its district

courts to dismiss data breach cases for lack of standing unless plaintiffs allege actual misuse of the hacked data or specifically allege how such misuse is certainly impending."); Allison v. Aetna, Inc., Civ. No. 09-2560, 2010 WL 3719243, at *4-5 (E.D. Pa. Mar. 9, 2010) (finding the "*mere possibility* of increased risk of identity theft" insufficient to confer standing) (emphasis in original).

Conclusion

For the reasons stated here and those discussed on the record during oral argument, Defendant's motion to dismiss for lack of standing will be granted.

An appropriate Order will issue.

Dated: June 5, 2018

/s/ Joseph H. Rodriguez
Hon. Joseph H. Rodriguez
U.S.D.J.